

REMARKS/ARGUMENTS

In response to the Examiner's Office Action of February 17, 2006 the Applicant respectfully submits the accompanying Amendment to the claims and the below Remarks.

Regarding Amendment

In the Amendment:

page 1 of the specification is amended to delete the contents of line 1 and to insert the continuity details thereof into a new Cross-Reference to Related Applications section immediately under the title together with the patent number of the cross-referenced parent application;

claim 3 is amended to omit the recitation "to next in sequence"; and

claims 1, 2, 4 and 5 are unchanged.

It is respectfully submitted that the above amendments do not add new matter to the present application.

Regarding Priority

It is respectfully submitted that the subject matter of claimed invention is disclosed by the parent application, USSN 09/516,874, for at least the following reasons.

The subject matter of the claimed invention is disclosed, for example, at page 42, line 15-page 45, line 21 and page 92, line 31-page 93, line 31 of the specification of the parent application, where the claimed integrated circuit is clearly understood by one of ordinary skill in the art to be the disclosed authentication chips and the claimed accessory of the claimed invention is clearly understood by one of ordinary skill in the art to be the disclosed consumable, such as a car key or toner cartridge.

Regarding Specification

It is respectfully submitted that the above-described amendment to page 1 of the specification to insert the patent number of parent applications, provides the amendment required by the Examiner. A Petition to Claim Priority (including fee) and a Replacement Declaration are enclosed.

Regarding 35 USC 112, second paragraph Rejections

It is respectfully submitted that the above-described amendment to claim 3 to omit the 1 of the recitation "to next in sequence", removes the antecedent basis problem raised by the Examiner.

Regarding 35 USC 102 and 103 Rejections

Regarding Doljack (US 6,442,276)

It is respectfully submitted that the subject matter of pending claims 1, 2, 4 and 5 and amended claim 3 is not taught or suggested by Doljack, for at least the following reasons.

The claimed invention is directed to the described "protocol 3" in which two secret keys K_1 and K_2 are employed to ensure that no correlation between a one-way function $F[R]$ based on the secret key K_1 and a one-way function $F[R|M]$ based on the secret key K_2 . In this way, the authentication chip of an accessory, such as a consumable (e.g., an electronic car key), can be advantageously securely authenticated (see page 42, line 15-page 45, line 21 and page 92, line 31-page 93, line 31 of the present specification).

On the other hand, Doljack merely describes employing a private/public key pair to encrypt random number sequences for the unique labelling of goods. That is, only a single secret key is used in the process disclosed by Doljack (see col. 8, lines 15-61 of Doljack).

The Examiner asserts that the one-way hash function disclosed by Doljack at col. 11, lines 9-22, constitutes a second secret key. The Applicant respectfully disagrees, because one of ordinary skill in the art clearly understands that this is not the case as is discussed at http://en.wikipedia.org/wiki/Secret_key, <http://en.wikipedia.org/wiki/HMAC>, and at page 13, line 30-page 18, line 6 of the present specification. That is, it is well known that a one-way hash function must be further combined with a secret key to result in a keyed hash function.

Further, there is no motivation from the disclosure of Doljack for one of ordinary skill in the art to modify the disclosed process to use a second secret key, this is because Doljack clearly discloses that the combination codes which combine random number generation, a private/public key pair and a one-way hash function, provides sufficient security for the unique goods labels (see col. 6, line 62-col. 7, line 64, col. 9, line 51-col. 10, line 21 and col. 11, lines 9-22 of Doljack).

Thus, the subject matter of pending independent claims 1 and 5, and dependent claims 2-4, is not taught or suggested by Doljack.

Regarding Ford et al. (in Secure Electronic Commerce) and Schneier et al. (US 6,099,408)

It is respectfully submitted that the subject matter of pending claims 1, 2, 4 and 5 and amended claim 3 is not taught or suggested by Ford or Schneier, for at least the above-discussed and following reasons.

The Examiner asserts that the hash functions disclosed by Ford (at page 129, section b) and Schneier (at col. 11, line 17-col. 12, line 3) constitutes a secret key. However, as discussed above it is well known that a one-way hash function must be further combined with a secret key to result in a keyed hash function.

The Examiner takes official notice that duplicating the disclosed processes using a single secret key (even though using a secret key is not disclosed by either Ford nor Schneier), thereby using a second secret key, would have been obvious, even though Ford and Schneier fail to disclose using a second secret key. However, the claimed invention does not involve duplicating a process using a single secret key. Rather, as clearly claimed, the two, different secret keys are used to provide different parameters respectively used to define a function based on random number generation and a test function used to compare read parameters with the defined parameters.

Thus, the subject matter of pending independent claims 1 and 5, and dependent claims 2-4, is not taught or suggested by Ford or Schneier.

It is respectfully submitted that all of the Examiner's objections and rejections have been traversed. Accordingly, it is submitted that the present application is in condition for allowance and reconsideration of the present application is respectfully requested.

Very respectfully,

Applicant:



KIA SILVERBROOK

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com
Telephone: +612 9818 6633
Facsimile: +61 2 9555 7762

Petition to Accept an Unintentionally Delayed Claim under 35 U.S.C. 120

The Applicant hereby petitions to accept an unintentionally delayed claim under 35 U.S.C. 120 for the benefit of a prior-filed application in accordance with 37 C.F.R. 1.78(a)(3).

- With respect to 37 C.F.R. 1.78(a)(3)(i), the reference required by 35 U.S.C. 120 and 37 C.F.R. 1.78(a)(2) is being concurrently filed herewith;
- With respect to 37 C.F.R. 1.78(a)(3)(ii), the surcharge set forth in 37 C.F.R. 1.17(t) is being submitted herewith; and
- With respect to 37 C.F.R. 1.78(a)(3)(iii), it is submitted that the entire delay between the date the claim was due under 37 C.F.R. 1.78(a)(2)(ii) and the date the claim is being filed concurrently herewith was unintentional.

It is hereby submitted that this petition is timely filed and meets the priority claim referred to by the Examiner in the Office Action dated February 17, 2006.

Very respectfully,

Applicant:



KIA SILVERBROOK

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com
Telephone: +612 9818 6633
Facsimile: +61 2 9555 7762